

LOGISTICS PKI SERVICE SYSTEM, PORTABLE TERMINAL, AND LOGISTIC PKI SERVICE METHOD USED THEREFOR

Publication number: JP2003223493 (A)

Publication date: 2003-08-08

Inventor(s): KATAYAMA TORU; YOSHIDA YOSHINORI +

Applicant(s): NEC CORP +

Classification:

- International: B65G61/00; G06K1/12; G06K17/00; G06K19/00; G06K19/10; G06K7/00; G06Q10/00; G06Q20/00; G06Q50/00; G09F3/00; H04L9/32; B65G61/00; G06K1/00; G06K17/00; G06K19/00; G06K19/10; G06K7/00; G06Q10/00; G06Q20/00; G06Q50/00; G09F3/00; H04L9/32; (IPC1-7): B65G61/00; G06F17/60; G06K1/12; G06K17/00; G06K19/00; G06K19/10; G06K7/00; G09F3/00; H04L9/32

- European: G06Q10/00D; G06Q20/00; G06Q20/00K1; G06Q20/00K3B; G06Q20/00K5

Application number: JP20020020841 20020130

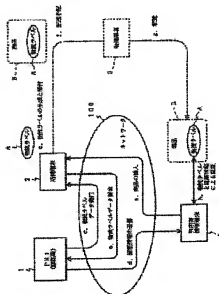
Priority number(s): JP20020020841 20020130

Also published as:

US2003144968 (A1)
US2008109247 (A1)
US2008183482 (A1)

Abstract of JP 2003223493 (A)

PROBLEM TO BE SOLVED: To provide a logistic PKI (Public key Infrastructure) service system capable of improving reliability and safety in a physical distribution part. **SOLUTION:** When an article released from a portable terminal 4 of a user to a store terminal 2 via a network 1000 is purchased, the store terminal 2 receives physical distribution label data issued from PKI 1 and the portable terminal of the user receives an identification information transmitted from the PKI 1. The store terminal 2 produces a physical distribution label A based on the physical distribution label data from the PKI 1, attaches the physical distribution label A to the article B, and requests the delivery of the article B to a physical distribution agent 3. When the article B is delivered by the physical distribution agent 3, the portable terminal 4 of the user reads information of the physical distribution label A attached to the article B and identifies it by the information of the physical distribution label A and the identification information from the PKI 1. ;
COPYRIGHT: (C)2003,JPO



Data supplied from the *espacenet* database — Worldwide

(11)特許出願公開番号
特開2003-223493
(P2003-223493A)

(43)公開日 平成15年8月8日(2003.8.8)

| (51) Int.CL ⁷ | 識別番号 | F I | データベース ^(参考) |
|--------------------------|----------------|---------------|------------------------------------|
| G 0 6 F 17/60 | 1 1 4 5 1 2 | G 0 6 F 17/60 | 1 1 4 5 B 0 3 3 5 1 2 5 B 0 5 8 |
| B 6 5 G 61/00 | 5 2 4 5 5 0 | B 6 5 G 61/00 | 5 2 4 5 B 0 7 2 5 5 0 5 J 1 0 4 |
| G 0 6 K 1/12 | | G 0 6 K 1/12 | A |

審査請求 未請求 請求項の数24 O L (全 16 頁) 最終頁に続く

審査請求 未請求 請求項の数24 OL (全 16 頁) 最終頁に続く

(21) 出願番号 特願2002-20841(P2002-20841)

(22) 出願日 平成14年1月30日(2002.1.30)

(71)出題人 000004237

日本電気株式会社
東京都港区芝五丁目7番1号

(72) 究明者 片山 透

東京都港区芝五丁目7番1号 日本電気株式会社内

(72)発明者 吉田 吉憲

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100088812

弁理士 ▲柳▽川 信

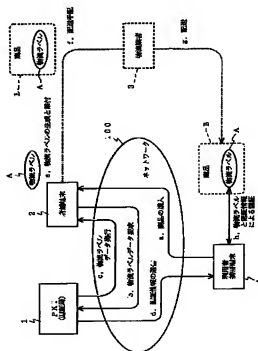
[最終頁に続く](#)

(54) 【発明の名称】 ロジスティックPKIサービスシステム、携帯端末及びそれに用いるロジスティックPKIサービス方法

(57) 【要約】

【課題】 物流部分における信頼性や安全性を向上可能なロジスティックPKIサービスシステムを提供する。

【解決手段】 利用者の携帯端末4からネットワーク100を介して店舗端末2に指示された商品が購入されると、店舗端末2はPKI1から発行される物流ラベルデータを受取り、利用者の携帯端末4はPKI1から送信される認証情報を受信する。店舗端末2はPKI1からの物流ラベルデータに基づいて物流ラベルAを生成し、その物流ラベルAを商品Bに添付した後、商品Bの配送依頼を物流業者3に依頼する。利用者の携帯端末4は物流業者3によって商品Bの情報が送られると、商品Bに添付された物流ラベルAの情報を受取り、物流ラベルAの情報とPKI1からの認証情報とによる認証を行う。



【特許請求の範囲】

【請求項1】 配送物の配送時に当該配送物の情報を示すラベルデータを要求しかつ送られてきた前記ラベルデータに基づいて前記配送物に添付するラベルを生成する端末装置と、

前記端末装置からの要求に応答して前記ラベルデータと前記配送物の認証情報とを発行する認証局と、
配送されてきた前記配送物に添付されている前記ラベルから読取った情報と前記認証局からの前記認証情報とによって認証を行う携帯端末とを有することを特徴とするロジスティックPKIサービスシステム。

【請求項2】 前記ラベルは、少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを示す情報を含むことを特徴とする請求項1記載のロジスティックPKIサービスシステム。

【請求項3】 前記ラベルは、前記配送物の受取者の公開鍵で暗号化され、前記配送物の受取時に前記配送物の受取者の秘密鍵で復号されることを特徴とする請求項2記載のロジスティックPKIサービスシステム。

【請求項4】 前記ラベルは、二次元バーコードとして印刷されることを特徴とする請求項2または請求項3記載のロジスティックPKIサービスシステム。

【請求項5】 前記ラベルは、集積回路からなるタグであることを特徴とする請求項2または請求項3記載のロジスティックPKIサービスシステム。

【請求項6】 前記認証局は、前記配送物の配送元を証明する電子署名を発行する手段と、前記配送物の依頼者を証明する電子署名を発行する手段とを含むことを特徴とする請求項1から請求項5のいずれか記載のロジスティックPKIサービスシステム。

【請求項7】 前記携帯端末は、前記配送物の認証結果として少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを前記ラベルから復号して表示することを特徴とする請求項2から請求項5のいずれか記載のロジスティックPKIサービスシステム。

【請求項8】 前記配送物の依頼者と前記配送物の受取者とが同一であることを特徴とする請求項1から請求項7のいずれか記載のロジスティックPKIサービスシステム。

【請求項9】 前記配送物の依頼者と前記配送物の受取者とが異なることを特徴とする請求項1から請求項7のいずれか記載のロジスティックPKIサービスシステム。

【請求項10】 配送されてきた配送物に添付されている当該配送物の情報を示すラベルから読取った情報と認証局からの当該配送物の認証情報とによって認証を行う手段を有することを特徴とする携帯端末。

【請求項11】 前記ラベルは、少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを示す情報を含むことを特徴とする請求項10記載の

携帯端末。

【請求項12】 前記ラベルは、前記配送物の受取者の公開鍵で暗号化され、前記配送物の受取時に前記配送物の受取者の秘密鍵で復号されることを特徴とする請求項11記載の携帯端末。

【請求項13】 前記ラベルは、二次元バーコードとして印刷されることを特徴とする請求項11または請求項12記載の携帯端末。

【請求項14】 前記ラベルは、集積回路からなるタグであることを特徴とする請求項11または請求項12記載の携帯端末。

【請求項15】 前記配送物の認証結果として少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを前記ラベルから復号して表示するようにしたことを特徴とする請求項1から請求項14のいずれか記載の携帯端末。

【請求項16】 端末装置において、配送物の配送時に当該配送物の情報を示すラベルデータを要求し、それに応答して送られてきた前記ラベルデータに基づいて前記配送物に添付するラベルを生成し、認証局において、前記端末装置からの要求に応答して前記ラベルデータと前記配送物の認証情報とを発行し、

携帯端末において、配送されてきた前記配送物に添付されている前記ラベルから読取った情報と前記認証局からの前記認証情報とによって認証を行うことを特徴とするロジスティックPKIサービス方法。

【請求項17】 前記ラベルは、少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを示す情報を含むことを特徴とする請求項16記載のロジスティックPKIサービス方法。

【請求項18】 前記ラベルは、前記配送物の受取者の公開鍵で暗号化され、前記配送物の受取時に前記配送物の受取者の秘密鍵で復号されることを特徴とする請求項17記載のロジスティックPKIサービス方法。

【請求項19】 前記ラベルは、二次元バーコードとして印刷されることを特徴とする請求項17または請求項18記載のロジスティックPKIサービス方法。

【請求項20】 前記ラベルは、集積回路からなるタグであることを特徴とする請求項17または請求項18記載のロジスティックPKIサービス方法。

【請求項21】 前記認証局において、前記配送物の配送元を証明する電子署名を発行し、前記配送物の依頼者を証明する電子署名を発行することを特徴とする請求項16から請求項20のいずれか記載のロジスティックPKIサービス方法。

【請求項22】 前記携帯端末において、前記配送物の認証結果として少なくとも前記配送物の配送元と、前記配送物の依頼者と、前記配送物の内容とを前記ラベルから復号して表示することを特徴とする請求項17から請求項20のいずれか記載のロジスティックPKIサービス

ス方法。

【請求項23】 前記配送物の依頼者と前記配送物の受取者とが同一であることを特徴とする請求項16から請求項22のいずれかが記載のロジスティックPKIサービス方法。

【請求項24】 前記配送物の依頼者と前記配送物の受取者とが異なることを特徴とする請求項16から請求項22のいずれかが記載のロジスティックPKIサービス方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はロジスティックPKIサービスシステム、携帯端末及びそれに用いるロジスティックPKIサービス方法に関し、特に物流を伴うエレクトリックコマースに代表されるPKI (Public Key Infrastructure) サービスに関する。

【0002】

【従来の技術】 近年、インターネットの普及に伴って、エレクトリックコマースに代表されるサービス、つまり通信販売等を代表とする物流を伴うサービスが普及してきている。このサービスは、主に商品の注文機能や代金の決済機能を電子的に支援するものである。

【0003】 さらに、携帯電話やPDA (Personal Digital Assistants) 等の携帯端末を用いたモバイルEC (Electronic Commerce) も普及してきており、インターネットでのエレクトリックコマースにおいて、ネットワーク上の機能を提供するシステム（サービス）は多数存在する。

【0004】

【発明が解決しようとする課題】 しかしながら、上述した従来のネットワーク上の機能を提供するシステムでは、インターネット上で商品を購入しても、実際には物流システムによってその商品が配送されているので、配達された商品が正当な送り主から送付されたのか、あるいは実際に注文した商品が送付されたのかを確認する作業を、商品を目で確認し、受領証に印鑑を捺印することで行わなければならない、配送時のトラブルが発生する恐れがある。

【0005】 この場合、配送時のトラブルとしては商品の誤配、誰から送られてきたか分からないという差出人の不明、依頼品の確認を行うことができない等、宅配や一般の郵便（書留等）、通信販売、エレクトリックコマース等の物流部分における信頼性や安全性を確保することができないという問題がある。

【0006】 したがって、従来のエレクトリックコマースでは、上述したような物流に伴う作業を電子的にサポートする機能を提供していないので、旧来の通信販売以上に普及していない。

【0007】 そこで、本発明の目的は上記の問題点を解

消し、物流部分における信頼性や安全性を向上させることができるロジスティックPKIサービスシステム、携帯端末及びそれに用いるロジスティックPKIサービス方法を提供することにある。

【0008】

【課題を解決するための手段】 本発明によるロジスティックPKIサービスシステムは、配送物の配送時に当該配送物の情報を示すラベルデータを要求しかつ送られてきた前記ラベルデータに基づいて前記配送物に添付するラベルを生成する端末装置と、前記端末装置からの要求にตอบสนองして前記ラベルデータと前記配送物の認証情報とを発行する認証局と、配送されてきた前記配送物に添付されている前記ラベルから読取った情報と前記認証局からの前記認証情報とによって認証を行う携帯端末とを備えている。

【0009】 本発明による携帯端末は、配送されてきた前記配送物に添付されているラベルから読取った情報と認証局からの当該配送物の認証情報とによって認証を行う手段を備えている。

【0010】 本発明によるロジスティックPKIサービス方法は、端末装置において、配送物の配送時に当該配送物の情報を示すラベルデータを要求し、それに応じて送られてきた前記ラベルデータに基づいて前記配送物に添付するラベルを生成し、認証局において、前記端末装置からの要求にตอบสนองして前記ラベルデータと前記配送物の認証情報とを発行し、携帯端末において、配送されてきた前記配送物に添付されている前記ラベルから読取った情報と前記認証局からの前記認証情報とによって認証を行っている。

【0011】 すなわち、本発明のロジスティックPKI (Public Key Infrastructure) サービスシステムは、店舗や郵便局等の端末装置が配送物の配送が依頼された時に当該配送物の情報を示すラベルデータを認証局に要求し、認証局がその要求にตอบสนองしてラベルデータと当該配送物の認証情報とを発行し、店舗や郵便局等の端末装置が認証局からのラベルデータに基づいてラベルを生成して配送物に添付し、利用者の携帯端末が配送されてきた配送物に添付されているラベルから読取った情報と認証局からの認証情報とによって、利用者の、配送物、店舗や郵便局等の認証を行うようにしている。

【0012】 上記のように構成することで、本発明のロジスティックPKIサービスでは、誤配を防止したり、差出人の確認や依頼品の確認（通信販売のケース）を公開鍵の証明書を含む電子署名にて電子的に行うことが可能となり、贈答品等の宅配や一般の郵便（書留等）、通信販売、エレクトリックコマース (E: Electronic Commerce) の物流部分における信頼性や安全性を向上させることが可能となる。

【0013】

【発明の実施の形態】次に、本発明の実施例について図面を参照して説明する。図1は本発明の第1の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。図1において、本発明の第1の実施例によるロジスティックPKIサービスシステムはPKI (Public Key Infrastructure) (認証局) 1と、店舗端末2と、利用者の携帯端末4とから構成されている。尚、このシステムの物流部分には店舗から利用者への商品の配送等を行う物流業者3が介在する。

【0014】既存の物流を伴うサービスとしては、エレクトリックコマース (EC: Electronic Commerce) (モバイルECを含む)、通信販売、贈答品等の一般の店舗での配送を伴う商品購入及びその宅配、一般の郵便 (書留等) がある。本実施例ではモバイルECについて説明する。

【0015】モバイルECには、一般的に、取引がネットワーク上で行われる「リモート環境」と、実際に店舗での取引が存在する「ローカル環境」とがある。本実施例では「リモート環境」におけるロジスティックPKIサービスシステムを示している。

【0016】一般に、「リモート環境」とは、モバイルECにおいて、上記のように、取引のほとんどがネットワークを通じて行われる環境のことである。例えば、オンラインショッピングによる商品購入等がこれにあたる。

【0017】本実施例はモバイルECの商品販売等での物流に伴う認証サービス、つまりロジスティックPKIサービスを提供するものである。ロジスティックPKIサービスはこれまでの物流において発生していた問題、つまり配送や郵送される物品、依頼者、配送元が正しいものかどうかを証明するものの確認を行えないという問題を解決し、信頼性や安全性を向上、顧客の満足度を飛躍的に向上させる。また、ロジスティックPKIサービスは既存の物流システムに比較的に適合可能なため、導入が容易である。

【0018】このロジスティックPKIサービスはこれまでのエレクトリックコマースサービスでは解決されていない、商取引における物流に関わるサービスであり、顧客の満足度を飛躍的に向上させ、エレクトリックコマースの市場を確実に拡大させる。

【0019】ロジスティックPKIサービスでは、モバイルECにおいて、ネットワーク100上で購入した商品Bを配送する際に、認証局1が発行した取引される商品Bに関する情報を物流ラベルAとして添付する。利用者が商品Bを物流業者3から受取る際に、その商品Bがどこから送られてきたのか、誰が注文したのか、商品Bは何なのか等の情報を電子的に証明する公開鍵の証明書を含む電子署名を、利用者の携帯端末4が物流ラベルAから読取り、それらを電子的に確認することが可能と

なる。

【0020】上述したサービスモデルは、ネットワーク100上で物品購入を想定した、いわゆるB2C (Business to Consumer) のモデルであり、利用者=商品の受取者、商品の送付者=店舗、物流業者=宅配業者である場合のモデルである。これ以外のモデルとして、同じB2Cでも、贈答品等のように利用者が注文者と受取者とはに分かれるモデル、一般郵便等のように店舗等が存在しないC2C (Consumer to Consumer) のモデルも考えられる。

【0021】いずれのモデルにおいても、利用者の携帯端末4、PKI (認証局) 1、物流業者3の下でロジスティックPKIサービスを利用することで、安全な物流システムを提供することが可能となる。尚、本モデルは既存の通信販売に適用した場合にも、ほぼ同じサービスモデルであると考えられる。

【0022】図2は図1の利用者の携帯端末4の構成を示すブロック図である。図2において、利用者の携帯端末4はネットワーク100上で商品Bを注文するための商品注文機能41と、ネットワーク100上で購入した商品Bの配送を依頼するための配送依頼機能42と、電子署名を生成する署名生成機能43と、物流ラベルAを読取る物流ラベル読取り機能44と、読取った物流ラベルAの情報を復号する復号機能45と、復号された物流ラベルAの情報に基づいて認証を行う認証機能46とを含んで構成されている。

【0023】尚、利用者の携帯端末4の他の機能として考えられる携帯電話の電話機能や、PDA (Personal Digital Assistants) のデータ処理機能等については公知であるので、その構成や動作についての説明は省略する。また、商品注文機能41や配送依頼機能42には物流ラベルAを生成するための情報を発信する機能を持つ場合もある。

【0024】図3は図1のPKI 1の構成を示すブロック図である。図3において、PKI 1は店舗の公開鍵等の証明書を含む電子署名を発行する店舗証明書発行機能11と、利用者の公開鍵等の証明書を含む電子署名を発行する利用者証明書発行機能12と、店舗証明書発行機能11及び利用者証明書発行機能12で発行された電子署名と店舗端末2からの商品情報とを基に物流ラベルデータを発行する物流ラベルデータ発行機能13と、店舗証明書発行機能11及び利用者証明書発行機能12で発行される電子署名や物流ラベルデータ発行機能13で発行される物流ラベルデータを暗号化する暗号化機能14とを含んで構成されている。

【0025】図4は図1の店舗端末2の構成を示すブロック図である。図4において、店舗端末2にはPKI 1に対する物流ラベルデータの発行要求やPKI 1からの物流ラベルデータの処理を行う物流ラベルデータ処理機

能21と、物流ラベルデータ処理機能21で処理した物流ラベルデータを印刷する物流ラベルデータ印刷機能22と、物流ラベルデータ印刷機能22で印刷された物流ラベルAを商品Bに添付する物流ラベル商品添付機能23とからなる物流ラベル処理装置と、電子署名を生成する署名生成機能24と、利用者の携帯端末4との間の通信を行う携帯端末間通信機能25とを含んで構成されている。

【0026】物流ラベルデータ処理機能21はネットワーク100を介してPKI1からデジタルデータとして送付されてくる物流ラベルデータを処理し、物流ラベルデータ印刷機能22は物流ラベルデータ処理機能21で処理された物流ラベルデータを物流ラベルAとして印刷する。物流ラベル商品添付機能23は物流ラベルデータ印刷機能22で印刷された物流ラベルAを商品Bに添付する。

【0027】尚、物流ラベル処理装置は店舗に置く場合、店舗の物流業者として一般の宅配業者が採用されていば、その宅配受付窓口の数だけ設置する。また、物流ラベル処理装置は物流業者3に設置することも可能である。

【0028】図5は本発明の第1の実施例によるロジスティックPKIサービスシステムの動作を示すシーケンスチャートである。これら図1～図5を参照して本発明の第1の実施例によるロジスティックPKIサービスシステムの動作について説明する。尚、以下の説明では、利用者が、店舗がそれぞれ秘密鍵を持ち、PKI1がそれらの秘密鍵に対する公開鍵を認証する公開鍵証明書電子署名として発行するものとする。

【0029】まず、利用者が携帯端末4の商品注文機能41や配送依頼機能42からネットワーク100を介して、店舗端末2に指示された商品Bの購入や当該商品Bの配送依頼を行うと（図1のa）（図5ステップS1）、店舗端末2は物流ラベルデータ処理機能21を用いて利用者の携帯端末4から入力される情報（利用者公開鍵・商品情報・商品情報への利用者秘密鍵による署名）を基にPKI1に物流ラベルデータの発行を要求する（図1のb）（図5ステップS2）。

【0030】PKI1はその物流ラベルデータの発行要求に応答して、店舗端末2から入力される情報（利用者公開鍵・商品情報・店舗公開鍵・商品情報への利用者秘密鍵による署名・注文ID・注文IDへの店舗秘密鍵による署名）を基に店舗証明書発行機能11にて店舗の公開鍵証明書を発行し（図5ステップS3）、物流ラベルデータ発行機能13にて商品情報への署名・注文IDへの署名を利用者の公開鍵で暗号化した物流ラベルデータを作成する（図5ステップS4）。

【0031】PKI1は作成した物流ラベルデータを店舗端末2に送信するとともに（図1のc）（図5ステップS5）、上記の情報（商品情報・注文ID・店舗の公

開鍵証明書）を暗号化機能14にて利用者の公開鍵を基に暗号化した認証情報を、利用者の携帯端末4に電子メール等を用いて送信する（図1のd）（図5ステップS6）。

【0032】店舗端末2はPKI1から発行される物流ラベルデータを受取ると、PKI1からの物流ラベルデータに基づいて物流ラベルAを生成し、その物流ラベルAを商品Bに添付した後（図1のe）（図5ステップS7）、商品Bの配送依頼を物流業者3に依頼する（図1のf）。

【0033】ここで、物流ラベルAとは店舗ID（店舗の公開鍵証明書そのものか、それから得られるID等）と、商品情報と、利用者ID（利用者の公開鍵証明書そのものか、それから得られるID等）または利用者が生成した電子署名とを利用者の公開鍵で暗号化した情報から生成された二次元バーコード、あるいはその情報を格納するICタグ等である。また、上述した公開鍵や公開鍵証明書の送信は全て、公開鍵や公開鍵証明書から得られるIDの送信に置き換えることができる。

【0034】利用者の携帯端末4はPKI1から送信される認証情報を受信し、物流業者3によって商品Bが配送されると（図1のg）（図5ステップS8）、物流ラベル読取り機能44にて商品Bに添付された物流ラベルAの情報を読取る（図5ステップS9）。

【0035】この場合、物流ラベル読取り機能44は物流ラベルAが二次元バーコードであれば、その二次元バーコードを読取るためのスキャナ機能が、物流業者の使用している端末のスキャナ機能にて二次元バーコードを読取った情報を受取るためのインターフェースを備え、物流ラベルAがICタグであれば、ICタグから情報を読取る機能を備えている。

【0036】利用者の携帯端末4は物流ラベル読取り機能44で読取った物流ラベルAの情報を復号機能45にて利用者の秘密鍵を基に復号し（図5ステップS10）、認証機能46にて物流ラベルAの情報とPKI1からの認証情報とによる認証を行う（図1のh）（図5ステップS11）。

【0037】ここで、認証機能46は物流ラベルAの情報とPKI1からの認証情報とを比較することで、物流ラベルAと認証情報とから得られる商品情報・注文ID・店舗の公開鍵証明書をそれぞれ検証、確認するとともに、その検証、確認の結果を図示せぬ画面上に表示する。

【0038】これによって、利用者はその商品Bがどこから送られてきたのか、誰が注文したのか、商品Bはどのような等の情報を、電子的に証明する公開鍵の証明書を含む電子署名にて電子的に確認することができる。

【0039】図6は本発明の第2の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。図6において、本発明の第2の実施例による

ロジスティックPKIサービスシステムは店舗での配送を伴う商品購入でのローカル環境のサービスモデルを示している。

【0040】尚、本発明の第2の実施例によるロジスティックPKIサービスシステムは店舗において配送を伴う商品購入を行う以外は図1に示す本発明の第1の実施例によるロジスティックPKIサービスシステムと同様の構成である。この場合、申込者及び受取者はネットワーク100を介することなく、上記の利用者の携帯端末4を用いて商品Bの購入申込み及び受取りを行う点以外は本発明の第1の実施例によるロジスティックPKIサービスシステムと同様である。

【0041】一般に、ローカル環境とはモバイルECにおいて、取引の一部が実際の店舗で行われる環境であり、例えば、モバイルを決済等に利用したコンビニエンスストアでの物品購入等がある。

【0042】ロジスティックPKIサービスでは、店舗での配送を伴う商品購入において、店舗で購入した商品Bを配送する際に、PKI1が発行しかつ取引される商品Bに関する情報を物流ラベルAとして添付する。受取者が商品Bを物流業者3から受取る際に、その商品Bがどこから送られてきたのか、誰が注文したのか、商品Bは何なのか等を電子的に証明する公開鍵の証明書を含む電子署名を携帯端末4によって物流ラベルAから読取り、それらを電子的に確認することが可能となる。

【0043】上述したサービスモデルは、店舗での物品購入を想定した、いわゆるB2Cのモデルであり、申込者＝商品の購入者、受取者＝商品の受取者、商品の送付者＝店舗、物流業者＝宅配業者である場合のモデルであり、申込者及び受取者の携帯端末4、PKI（認証局）1、物流業者3の下でロジスティックPKIサービスを利用することで、安全な物流システムを提供することが可能となる。尚、宅配やP2P（Peer to Peer）である一般の郵便（書留等）に適用した場合にもほぼ同じサービスモデルとなる。

【0044】本実施例において用いられる携帯端末4（申込者の携帯端末4a及び受取者の携帯端末4b）の構成は図2に示す本発明の第1の実施例の携帯端末4と同様の構成となっている。申込者の携帯端末4aでは配送依頼機能42を用いて店舗内のPOS（Point Of Sales）（図示せず）との間で通信を行い、店舗で購入した商品Bの配送を依頼する。

【0045】本実施例では店舗内のPOSが店舗端末2に相当し、配送依頼機能42は店舗端末2の携帯端末間通信機能25との間で通信を行うこととなる。これら配送依頼機能42と携帯端末間通信機能25との間での通信としては、非接触IC（集積回路）、IrDA（Infrared Data Association）、Bluetooth（R）等が考えられ、物流ラベルAを生成するための情報を発信する場合もある。

【0046】一方、受取者の携帯端末4bでは物流ラベル読取り機能44が物流ラベルAの情報を読取り、復号機能45が読取った物流ラベルAの情報を受取者の秘密鍵を用いて復号し、認証機能46が復号機能45で復号された物流ラベルAの情報に基づいて認証を行う。尚、申込者の携帯端末4a及び受取者の携帯端末4bの他の機能としては、図2に示す本発明の第1の実施例の携帯端末4と同様に、携帯電話の電話機能や、PDAのデータ処理機能等がある。

【0047】本実施例において用いられるPKI1の構成は図3に示す本発明の第1の実施例のPKI1と同様の構成となっている。このPKI1においては利用者証明書発行機能12による利用者の証明書が上記の携帯端末4の数（ n ）だけ必要となり、物流ラベルデータ発行機能13による物流ラベルデータの発行は物流トランザクション毎に発生することとなる。

【0048】本実施例において用いられる店舗端末2の物流ラベル処理装置の構成は図4に示す本発明の第1の実施例の店舗端末2と同様の構成となっている。物流ラベルデータの発行は上述したPKI1で行われるが、実際の商品Bへ物流ラベルAを添付するのは店舗または物流業者の物流ラベル処理装置で行われ、そのための装置が必要となる。

【0049】図7は本発明の第2の実施例によるロジスティックPKIサービスシステムの動作を示すシーケンスチャートである。これら図2～図4と図6と図7とを参照して本発明の第2の実施例によるロジスティックPKIサービスシステムの動作について説明する。尚、以下の説明では、申込者、受取者、店舗がそれぞれ秘密鍵を持ち、PKI1がそれらの秘密鍵に対する公開鍵を認証する公開鍵証明書を電子署名として発行するものとする。

【0050】まず、申込者が携帯端末4aの配送依頼機能42から店舗端末2の携帯端末間通信機能25を介して商品Bの配送依頼を行うと（図6のa）（図7ステップS21）、店舗端末2は物流ラベルデータ処理機能21を用いて利用者の携帯端末4から入力される情報（申込者公開鍵・受取者公開鍵・商品情報・商品情報への申込者秘密鍵による署名）を基にPKI1に物流ラベルデータの発行を要求する（図6のb）（図7ステップS22）。

【0051】PKI1はその物流ラベルデータの発行要求に応答して、店舗端末2から入力される情報（申込者公開鍵・受取者公開鍵・商品情報・商品情報への申込者秘密鍵による署名・店舗公開鍵・注文ID・注文IDへの店舗秘密鍵による署名）を基に店舗証明書発行機能11と利用者証明書発行機能12とを用いて申込者、店舗それぞれの公開鍵証明書を発行し（図7ステップS23）、物流ラベルデータ発行機能13にて商品情報への署名・注文IDへの署名を受取者の公開鍵で暗号化して

物流ラベルデータを作成する(図7ステップS24)。

【0052】PKI1は作成した物流ラベルデータを店舗端末2に送信するとともに(図6のc)(図7ステップS25)、上記の情報(商品情報・注文ID・申込者の公開鍵証明書・店舗の公開鍵証明書)を暗号化機能14にて受取者の公開鍵を基に暗号化した認証情報を、受取者の携帯端末4bに電子メール等を用いて送信する(図6のd)(図7ステップS26)。

【0053】店舗端末2はPKI1から発行される物流ラベルデータを受取ると、PKI1からの物流ラベルデータに基づいて物流ラベルAを生成し、その物流ラベルAを商品Bに添付した後(図6のe)(図7ステップS27)、商品Bの配送依頼を物流業者3に依頼する(図6のf)(図7ステップS28)。

【0054】ここで、物流ラベルAとは店舗ID(店舗の公開鍵証明書そのものか、それから得られるID等)と、商品情報と、申込者ID(申込者の公開鍵証明書そのものか、それから得られるID等)または申込者が生成した電子署名とを受取者の公開鍵で暗号化した情報から生成された二次元バーコード、あるいはその情報を格納するICタグ等である。また、上述した公開鍵や公開鍵証明書の送信は全て、公開鍵や公開鍵証明書から得られるIDの送信に置き換えることができる。

【0055】受取者の携帯端末4bはPKI1から送信される認証情報を受信し、物流業者3によって商品Bが配送されると(図6のg)(図7ステップS29)、物流ラベル読み取り機能44にて商品Bに添付された物流ラベルAの情報を读取する(図7ステップS30)。

【0056】この場合、物流ラベル読み取り機能44は物流ラベルAが二次元バーコードであれば、その二次元バーコードを读取するためのスキャナ機能が、物流業者の使用している端末のスキャナ機能にて二次元バーコードを读取した情報を受取るためのインタフェースを備え、物流ラベルAがICタグであれば、ICタグから情報を读取する機能を備えている。

【0057】受取者の携帯端末4bは物流ラベル読み取り機能44で读取した物流ラベルAの情報を復号機能45にて受取者の秘密鍵を基に復号し(図7ステップS31)、認証機能46にて物流ラベルAの情報とPKI1からの認証情報とによる認証を行う(図6のh)(図7ステップS32)。

【0058】ここで、認証機能46は物流ラベルAの情報とPKI1からの認証情報とを比較することで、物流ラベルAと認証情報とから得られる商品情報・注文ID・申込者の公開鍵証明書・店舗の公開鍵証明書をそれぞれ検証、確認するとともに、その検証、確認の結果を図示せぬ画面上に表示する。

【0059】これによって、受取者はその商品Bがどこから送られてきたのか、誰が注文したのか、商品Bは何なのか等の情報を、電子的に証明する公開鍵の証明書を

含む電子署名にて電子的に確認することができる。

【0060】図8は本発明の第3の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。図8において、本発明の第3の実施例によるロジスティックPKIサービスシステムは店舗での配送を伴う商品購入でのローカル環境のサービスモデルを示している。

【0061】尚、本発明の第3の実施例によるロジスティックPKIサービスシステムは申込者が携帯端末4aにてネットワーク100を介して店舗から商品購入を行う以外は図6に示す本発明の第2の実施例によるロジスティックPKIサービスシステムと同様の動作である。

【0062】図9は本発明の第4の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。図9において、本発明の第4の実施例によるロジスティックPKIサービスシステムは店舗での配送を伴う商品購入でのローカル環境のサービスモデルを示している。

【0063】尚、本発明の第4の実施例によるロジスティックPKIサービスシステムは受取者が電子的に確認した内容を申込者にネットワーク100を介して通知するように(図6に示す本発明の第2の実施例によるロジスティックPKIサービスシステムと同様の動作である)。

【0064】図10は本発明の第4の実施例によるロジスティックPKIサービスシステムの動作を示すシーケンスチャートである。図10において、ステップS21～S32は図7に示す本発明の第2の実施例によるロジスティックPKIサービスシステムの動作と同様であるので、その説明は省略する。

【0065】受取者の携帯端末4bは認証機能46による物流ラベルAの情報とPKI1からの認証情報とによる認証結果を申込者の携帯端末4aにネットワーク100を介して通知する(図9のi)(図10ステップS33)。この場合、受取者の携帯端末4bは復号機能45にて復号された物流ラベルAの情報と商品Bの受取り情報とを電子メール等で申込者の携帯端末4aに通知する。

【0066】よって、申込者は配送依頼を行った商品Bを受取者が受取ったことを電子的に確認することができる。尚、上述した本発明の第1～第4の実施例における物流ラベルAを用いることで、物流業者3による商品Bの配送状況をネットワーク100上で確認することも可能である。

【0067】図11は本発明の第5の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。図11において、本発明の第5の実施例によるロジスティックPKIサービスシステムは郵便(書留等)に適用した場合のサービスモデルを示しており、PKI(認証局)1と、郵便局端末5と、申込者の携帯

端末6a及び受取者の携帯端末6bとから構成されている。

【0068】上述した本発明の第1の実施例及び第2の実施例は、利用者が商品を店舗で購入して物流が発生するという点で、すべてB2Cである。しかしながら、本実施例による既存の郵便（書留等）への適用は、郵便という物流は伴うものの、商品自身が基本的に送り主、受取り主の所有物である点で、P2Pである。

【0069】ロジスティックPKIサービスでは、郵便物Dの郵送において、郵便局で依頼した郵便物Dを郵送する際に、PKI1が発行する郵送される郵便物Dに関する情報を郵便ラベルCとして添付する。受取者が郵便物Dを郵便事業者から受取る際に、その郵便物Dがどこから送られてきたのか、誰が郵送を依頼したのか等を、携帯端末6bによって郵便ラベルCから読取り、電子的に確認することが可能となる。

【0070】上述したサービスモデルは、郵便局を介した郵便物Dの郵送を想定した、いわゆるP2Pのモデルであり、申込者＝郵便物の郵送依頼者、受取者＝郵便物の受取者、郵便物の郵送者＝郵便事業者のモデルであり、申込者の携帯端末6a及び受取者の携帯端末6b、PKI1、郵便事業者の下でロジスティックPKIを利用することによって、安全な郵便システムを提供することが可能となる。尚、個人の依頼する年配に適用した場合にも、ほぼ同じサービスモデルとなる。

【0071】図12は図11の携帯端末6a、6bの構成を示すブロック図である。図7において、携帯端末6は郵便物の郵送を依頼する郵送依頼機能61と、電子署名を生成する署名生成機能43と、郵便ラベルCを読む郵便ラベル読取り機能62と、読取った郵便ラベルCの情報を復号する復号機能45と、復号された郵便ラベルCの情報に基づいて認証を行う認証機能46とを含んで構成されている。申込者の携帯端末6a及び受取者の携帯端末6bは上記の携帯端末6と同様の構成及び動作となっている。

【0072】尚、申込者の携帯端末6a及び受取者の携帯端末6bの他の機能として考えられる携帯電話の電話機能や、PDAのデータ処理機能等については公知であるので、その構成や動作についての説明は省略する。

【0073】また、郵送依頼機能61は郵便局内のPOS（図示せず）との間で通信を行い、郵便物Dの郵送を依頼する。この郵送依頼機能61としては非接触IC、IrDA、Bluetooth(R)等が考えられ、郵便ラベルCを生成するための情報を発信する場合もある。

【0074】図13は図11のPKI1の構成を示すブロック図である。図13において、PKI1は郵便局の公開鍵等の証明書を含む電子署名を発行する郵便局証明書発行機能15と、申込者及び受取者の公開鍵等の証明書を含む電子署名を発行する利用者証明書発行機能12

と、郵便局証明書発行機能15及び利用者証明書発行機能12で発行された電子署名と郵便局端末5からの郵便物情報とを基に郵便ラベルデータを発行する郵便ラベルデータ発行機能16と、郵便局証明書発行機能15及び利用者証明書発行機能12で発行される電子署名や郵便ラベルデータ発行機能16で発行される郵便ラベルデータを暗号化する暗号化機能14とを含んで構成されている。

【0075】このPKI1においては利用者証明書発行機能12による申込者及び受取者の証明書が上記の携帯端末6の数(×)だけ必要となり、郵便ラベルデータ発行機能16による郵便ラベルデータの発行は郵便トラザクション毎に発生することとなる。

【0076】図14は図11の郵便局端末5の構成を示すブロック図である。図14において、郵便局端末5にはPKI1に対する郵便ラベルデータの発行要求やPKI1からの郵便ラベルデータの処理を行う郵便ラベルデータ処理機能51と、郵便ラベルデータ処理機能51で処理した郵便ラベルデータを印刷する郵便ラベルデータ印刷機能52と、郵便ラベルデータ印刷機能52で印刷された郵便ラベルCを郵便物Dに添付する郵便ラベル郵便物添付機能53とからなる郵便ラベル処理装置と、電子署名を生成する署名生成機能54と、申込者の携帯端末6aとの間の通信を行う携帯端末間通信機能55とを含んで構成されている。郵便ラベルデータの発行は上述したPKI1で行われるが、実際の郵便物Dへ郵便ラベルCを添付するのは郵便局の郵便ラベル処理装置で行われる。

【0077】郵便ラベルデータ処理機能51はネットワーク100を介してPKI1からデジタルデータとして送付されてくる郵便ラベルデータを処理し、郵便ラベルデータ印刷機能52は郵便ラベルデータ処理機能51で処理された郵便ラベルデータを郵便ラベルCとして印刷する。郵便ラベル郵便物添付機能53は郵便ラベルデータ印刷機能52で印刷された郵便ラベルCを郵便物Dに添付する。

【0078】図15は本発明の第5の実施例によるロジスティックPKIサービスシステムの動作を示すシーケンスチャートである。これら図11～図15を参照して本発明の第5の実施例によるロジスティックPKIサービスシステムの動作について説明する。尚、以下の説明では、申込者、受取者、郵便局がそれぞれ秘密鍵を持ち、PKI1がそれらの秘密鍵に対する公開鍵を認証する公開鍵証明書を電子署名として発行するものとする。

【0079】まず、申込者は携帯端末6aを用いて郵便物Dの郵送依頼を行うと（図11のa）（図15ステップS41）、郵便局端末5は郵便ラベルデータ処理機能51を用いて申込者の携帯端末6aから入力される情報（申込者公開鍵・受取者公開鍵・郵便物情報・郵便物情報への申込者秘密鍵による署名）を基にPKI1に郵便

ラベルデータの発行を要求する(図11のb)(図15ステップS42)。

【0080】PKI1はその郵便ラベルデータの発行要求に応答して、郵便局端末5から入力される情報(申込者公開鍵・受取者公開鍵・郵便物情報・郵便物情報への申込者秘密鍵による署名・郵便局公開鍵・郵便ID・郵便IDへの郵便局秘密鍵による署名)を基に郵便局証明書発行機能15と利用者証明書発行機能12とを用いて申込者、郵便局それぞれの公開鍵証明書を発行し(図15ステップS43)、郵便ラベルデータ発行機能16にて郵便物情報への署名・郵便IDへの署名を受取者の公開鍵で暗号化して郵便ラベルデータを作成する(図15ステップS44)。

【0081】PKI1は作成した郵便ラベルデータを郵便局端末5に送信するとともに(図11のc)(図15ステップS45)、上記の情報(郵便物情報・郵便ID・申込者の公開鍵証明書・郵便局の公開鍵証明書)を暗号化機能14にて受取者の公開鍵を基に暗号化し、受取者の携帯端末6bに電子メール等を用いて送信する(図11のd)(図15ステップS46)。

【0082】郵便局端末5はPKI1から発行される郵便ラベルデータを受取ると、PKI1からの郵便ラベルデータに基づいて郵便ラベルCを生成し、その郵便ラベルCを郵便物Dに添付した後(図11のe)(図15ステップS47)、郵便物Dの郵送を行う(図11のf)(図15ステップS48)。

【0083】ここで、郵便ラベルCとは郵便局ID(郵便局の公開鍵証明書そのものか、それから得られるID等)と、郵便物情報と、申込者ID(申込者の公開鍵証明書そのものか、それから得られるID等)または申込者が生成した電子署名とを受取者の公開鍵で暗号化した情報から生成された二次元バーコード、あるいはその情報を格納するICタグ等である。また、上述した公開鍵や公開鍵証明書の送信は全て、公開鍵や公開鍵証明書から得られるIDの送信に置き換えることができる。

【0084】受取者の携帯端末6bはPKI1から送信される認証情報を受信し、郵便局から郵便物Dが郵送されると、郵便ラベル読取り機能62にて郵便物Dに添付された郵便ラベルCの情報を読取る(図15ステップS49)。

【0085】この場合、郵便ラベル読取り機能62は郵便ラベルCが二次元バーコードであれば、その二次元バーコードを読取るためのスキャナ機能か、郵便局員の使用している端末のスキャナ機能にて二次元バーコードを読取った情報を受取るためのインタフェースかを備え、郵便ラベルCがICタグであれば、ICタグから情報を読取る機能を備えている。

【0086】受取者の携帯端末6bは郵便ラベル読取り機能62で読取った郵便ラベルCの情報を復号機能45にて受取者の秘密鍵を基に復号し(図15ステップS5

0)、認証機能46にて郵便ラベルCの情報とPKI1からの認証情報とによる認証を行う(図11のh)(図15ステップS51)。

【0087】ここで、認証機能46は郵便ラベルCの情報とPKI1からの認証情報とを比較することで、郵便ラベルCと認証情報とから得られる郵便物情報・郵便ID・申込者の公開鍵証明書・郵便局の公開鍵証明書をそれぞれ検証、確認するとともに、その検証、確認の結果を図示せぬ画面上に表示する。

【0088】これによって、受取者はその郵便物Cが誰から送られてきたのか、郵便物Dは何なのか等の情報を、電子的に証明する公開鍵の証明書を含む電子署名にて電子的に確認することができる。

【0089】

【発明の効果】以上説明したように本発明は、認証局が、配送物の配送が依頼された時に当該配送物の情報を示すラベルデータと当該配送物の認証情報とを発行し、端末装置が、認証局からのラベルデータに基づいてラベルを生成して配送物に添付し、携帯端末が、配送されてきた配送物に添付されているラベルから読取った情報と認証局からの認証情報とによって認証を行うことによって、物流部分における信頼性や安全性を向上させることができるという効果が得られる。

【図面の簡単な説明】

【図1】本発明の第1の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。

【図2】図1の利用者携帯端末の構成を示すブロック図である。

【図3】図1のPKIの構成を示すブロック図である。

【図4】図1の店舗端末の構成を示すブロック図である。

【図5】本発明の第1の実施例によるロジスティックPKIサービスシステムの動作を示すシーケンスチャートである。

【図6】本発明の第2の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。

【図7】本発明の第2の実施例によるロジスティックPKIサービスシステムの動作を示すシーケンスチャートである。

【図8】本発明の第3の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。

【図9】本発明の第4の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。

【図10】本発明の第4の実施例によるロジスティックPKIサービスシステムの動作を示すシーケンスチャートである。

【図11】本発明の第5の実施例によるロジスティックPKIサービスシステムの構成を示すブロック図である。

【図12】図11の携帯端末の構成を示すブロック図で

ある。

【図13】図11のPKIの構成を示すブロック図である。

【図14】図11の郵便局端末の構成を示すブロック図である。

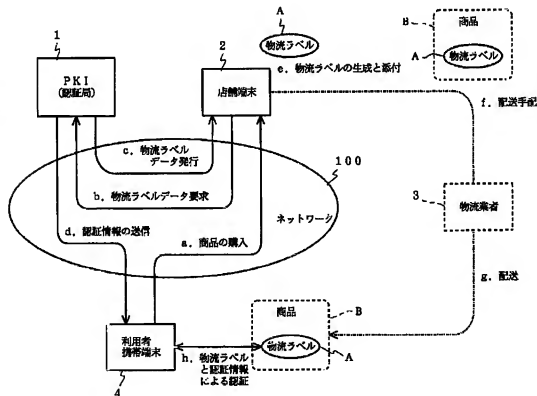
【図15】本発明の第5の実施例によるロジスティックPKIサービシステムの動作を示すシーケンスチャートである。

【符号の説明】

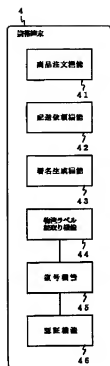
- 1、PKI
- 2、店舗端末
- 3、物流業者
- 4、4a、4b、
- 6、6a、6b 携帯端末
- 5 郵便局端末
- 11 店舗証明書発行機能
- 12 利用者証明書発行機能
- 13 物流ラベルデータ発行機能
- 14 暗号化機能
- 15 郵便局証明書発行機能
- 16 郵便ラベルデータ発行機能

- 21 物流ラベルデータ処理機能
- 22 物流ラベルデータ印刷機能
- 23 物流ラベル商品添付機能
- 24、43、54 署名生成機能
- 25、55 携帯端末間通信機能
- 41 商品注文機能
- 42 配送依頼機能
- 44 物流ラベル読取り機能
- 45 復号機能
- 46 認証機能
- 51 郵便ラベルデータ処理機能
- 52 郵便ラベルデータ印刷機能
- 53 郵便ラベル郵便物添付機能
- 61 郵送依頼機能
- 62 郵便ラベル読取り機能
- 100 ネットワーク
- A 物流ラベル
- B 商品
- C 郵便ラベル
- D 郵便物

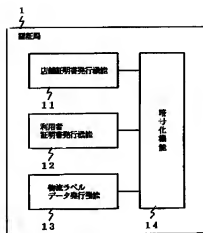
【図1】



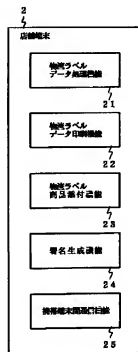
【図2】



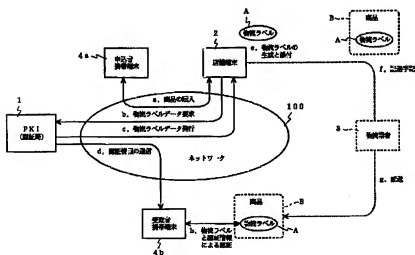
【図3】



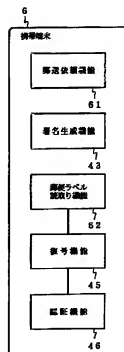
【図4】



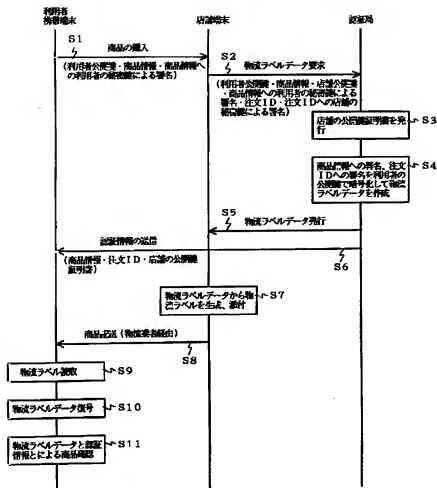
【図8】



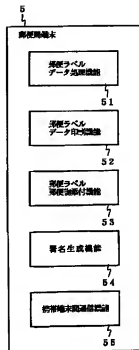
【図12】



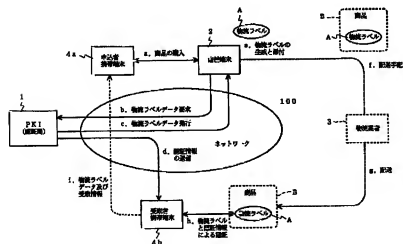
【図5】



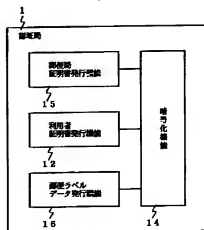
【図14】



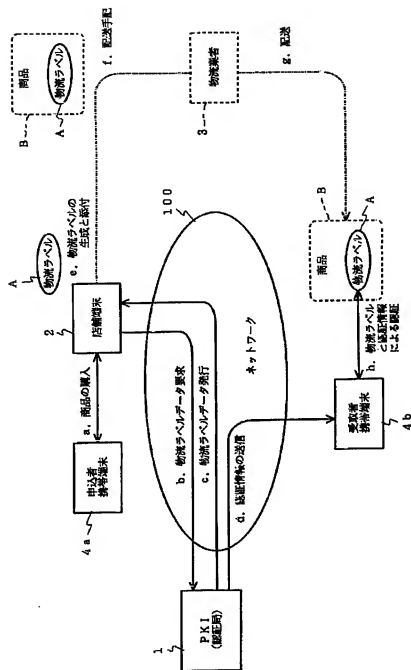
【図9】



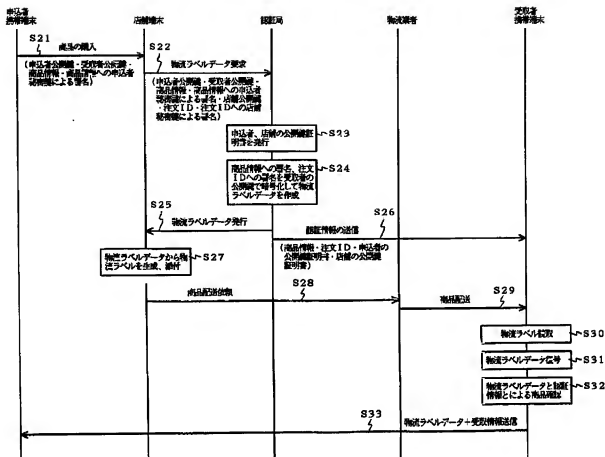
【図13】



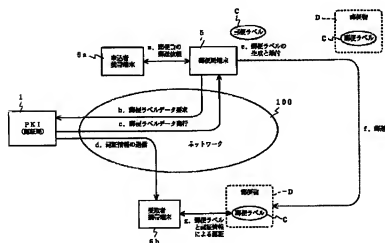
【図6】



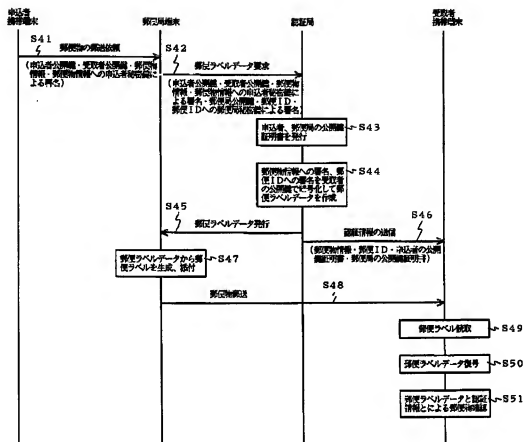
【図10】



【図11】



【图15】



フロントページの続き

| | | | |
|----------------------------|-------|---------------|---------|
| (51) Int. Cl. ⁷ | 識別記号 | F I | (参考) |
| G 0 6 K 7/00 | | G 0 6 K 7/00 | U |
| 17/00 | | 17/00 | L |
| | | | T |
| 19/00 | | G 0 9 F 3/00 | Z E C M |
| 19/10 | | H 0 4 L 9/00 | 6 7 5 D |
| G 0 9 F 3/00 | Z E C | | 6 7 5 B |
| H 0 4 L 9/32 | | G 0 6 K 19/00 | Q |
| | | | R |

Fチーム(参考) 5B035 AA13 BB01 BB09 BB11 BC00
CA23
5B058 CA15 KA02 KA06 KA11 KA35
YA20
5B072 BB00 CC06 CC24 DD01 GG01
GG07
5J104 AA10 KA05 MA01 PA10